UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/741,603	12/19/2000	Douglas G. Murray	END9-2000-0163US1	4760

23550 7590 05/16/2005

HOFFMAN WARNICK & D'ALESSANDRO, LLC
3 E-COMM SQUARE
ALBANY, NY 12207

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 05/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/741,603	MURRAY, DOUGLAS G.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-9* is/are allowed.

6)☒ Claim(s) *10-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 1-9 has been considered and found to be persuasive. The rejection of claims 1-9 under 35 USC 102(b) as being anticipated by Coppersmith et al has been withdrawn.

2. The applicant is correct in identifying claims 10-37 as not being addressed by the examiner. The examiner apologizes for inadvertently overlooking these claims.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 10-37 are rejected under 35 U.S.C. 102(b) as being anticipated by Coppersmith et al, U.S. Patent 5,768,390.

As per claims 10 and 27, Coppersmith et al teaches of a method and system for processing a data set that comprises the steps of providing input blocks (data set) being 64 bit values (first length)(col. 3, lines 29-33 and col. 4, lines 57-59). It is implied that

the key is formatted to a first length since they key is a 56 bit value (col. 4, lines 62-63). A masked key (formed by setting predetermined bits of the formatted key to zero) is used with the data set by forming an exclusive-OR result to yield an encrypted data set (col. 3, lines 33-40 and col. 4, lines 65-66). It is recited of 64 bit input block values (col. 4, lines 57-59) and they are gonna have higher and lower order bits since its more than 8 bits that which would include 4 higher order bits and 4 lower order bits. Since masking is used, it is interpreted by the examiner that the 4 higher order bits are set to zero since masking is used as a means to screen out certain bits by using logical operators (AND operation with binary 0000 and 1111).

As per claims 11-14, it is taught by Coppersmith et al that a key is masked and ultimately encrypted (col. 3, lines 33-36). Coppersmith et al teaches of 64 bit input block values (col. 4, lines 57-59) and they are gonna have higher and lower order bits since its more than 8 bits that which would include 4 higher order bits and 4 lower order bits. Since masking is used, it is interpreted by the examiner that the 4 higher order bits are set to zero since masking is used as a means to screen out certain bits by using logical operators (AND operation with binary 0000 and 1111).

As per claim 15, Coppersmith et al discloses of decrypting the encrypted data set by forming an inverse exclusive-OR result of the encrypted data set with the masked key (col. 4, line 66 through col. 5, line 8 and col. 6, lines 65-67).

As per claim 16, it is disclosed by Coppersmith et al of a second data set with a 64 bit (second length) value that is equal to the first length which is masked (truncated)(col. 3, lines 29-44 and col. 4, lines 57-59).

As per claims 17 and 28, the teachings of Coppersmith et al recite of using 64 bit input block values to yield encrypted data sets (col. 4, lines 57-59). It is interpreted that these values are in the printable ASCII range since they use binary digits of 1's and 0's to make of the bit values.

As per claims 18 and 29, Coppersmith et al discloses of a system and a program product stored on a recordable media for processing a data set having a first length for processing a data set that comprises the steps of providing input blocks (data set) being 64 bit values (first length)(col. 3, lines 29-33 and col. 4, lines 7-13,57-59). It is implied that the key is formatted to a first length since they key is a 56 bit value (col. 4, lines 62-63). A masked key (formed by setting predetermined bits of the formatted key to zero) is used with the data set by forming an exclusive-OR result to yield an encrypted data set (col. 3, lines 33-40 and col. 4, lines 65-66). The examiner is interpreting masking a being a process of setting predetermined bits of the formatted key to zero since masking is known as a binary value used to screen out certain bits in data by using logical operators.

As per claims 19,21,22,23,30,32,33, and 34, it is taught by Coppersmith et al that a key is masked and ultimately encrypted (col. 3, lines 33-36). Coppersmith et al teaches of 64 bit input block values (col. 4, lines 57-59) and they are gonna have higher and lower order bits since its more than 8 bits that which would include 4 higher order bits and 4 lower order bits. Since masking is used, it is interpreted by the examiner that the 4 higher order bits are set to zero since masking is used as a means to screen out certain bits by using logical operators (AND operation with binary 0000 and 1111).

As per claims 20 and 31, it is disclosed by Coppersmith et al of a second data set with a 64 bit (second length) value that is equal to the first length which is masked (truncated)(col. 3, lines 29-44 and col. 4, lines 57-59).

As per claims 24 and 35, Coppersmith et al discloses of using (replacing) the encrypted data set once the data set has been encrypted (col. 1, lines 16-22). A key is masked and ultimately encrypted (col. 3, lines 33-36). Coppersmith et al teaches of 64 bit input block values (col. 4, lines 57-59) and they are gonna have higher and lower order bits since its more than 8 bits that which would include 4 higher order bits and 4 lower order bits

As per claims 25 and 36, Coppersmith et al discloses of decrypting the encrypted data set by forming an inverse exclusive-OR result of the encrypted data set with the masked key (col. 4, line 66 through col. 5, line 8 and col. 6, lines 65-67).

As per claims 26 and 37, the teachings of Coppersmith et al recite of using 64 bit input block values to yield encrypted data sets (col. 4, lines 57-59). It is interpreted that these values are in the printable ASCII range since they use binary digits of 1's and 0's to make of the bit values.

Allowable Subject Matter

5. Claims 1-9 are allowed.

6. The following is a statement of reasons for the indication of allowable subject matter:

It was not found to be taught in the prior art of providing a data set having a first length, the first length may be of any length, formatting a key to match the first length, setting pre-determined bits of the formatted key to zero to yield a masked key, and forming an exclusive-OR result of the data set with the masked key to yield an encrypted data set.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131

5/12/05

CR

May 12, 2005